UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/552,780	10/12/2005	Thomas Andreas Maria Kevenaar	NL 031197	2050

24737 7590 12/08/2009

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
SCHWARTZ, DARREN B	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
12/08/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/552,780	KEVENAAR ET AL.	
	Examiner	Art Unit	
	DARREN SCHWARTZ	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 October 2005* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-27 are presented for examination.

Drawings

The drawings are objected to because the unlabeled figures shown in the drawings should be provided with descriptive labels.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

1. Claim 18 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter in that it does not fall under any of the 4 statutory classes of inventions.

Applicant claim is clearly directed to a signal alone.

Transitory, propagating signals such as carrier waves are not within any of the four statutory categories (process, machine, manufacture or composition of matter). Therefore, a claim directed to computer instructions embodied in a signal is not statutory under 35 U.S.C. 101. *In re Nuijten*, 500 F.3d 1346, 1354 (Fed. Cir. 2007).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1, 9-11, 13-17 and 19-25 are rejected under 35 U.S.C. 102(b) as being anticipated by D'Amico et al (U.S. Pat 5077790 A), hereinafter referred to as D'Amico.

Re claim 1: D'Amico teaches a method of secure device subscription, wherein a secret identifier ["key code"] and a public identifier ["portable identification number"] are stored in a subscribing device [Fig 1, elt 16: "SUSBSCRIBER UNIT"], the subscribing device subscribes itself to a subscription authority [Fig 1, elts 12 & 14; Fig 3; "BASE STATION" / "network operator"], involving

a step in which the subscribing device identifies itself with the public identifier (col 3, lines 4-10), and a step in which the subscription authority supplies subscription

information to the subscribing device (col 3, lines 10-18), characterized in that the method has

a first-time subscription protocol (Fig 4: col 2, lines 15-17) and a renewed subscription protocol (Fig 5: col 2, lines 18-19),

the subscription authority obtains a mapping of the secret identifier during execution of the first-time subscription protocol (col 1, lines 43-52), the subscription authority subsequently stores the mapping of the secret identifier (col 1, lines 43-52), and the subscription authority uses the stored mapping of the secret identifier during execution of the renewed subscription protocol [Fig 5a, elt 202] (col 4, lines 36-41).

Re claim 9: D'Amico teaches the first-time subscription protocol the subscribing device communicates the secret identifier to the subscription authority (Abstract, lines 30-33).

Re claim 10: D'Amico teaches during execution of any of the subscription protocols the subscription authority encrypts the subscription information using the secret identifier, and the subscription authority subsequently communicates the encrypted subscription information to the subscribing device (col 3, lines 50-55).

Re claim 11: D'Amico teaches the stored mapping of the secret identifier is the secret identifier itself (col 1, lines 44-52).

Re claim 13: D'Amico teaches execution of the renewed subscription protocol the subscription authority communicates the encrypted subscription information to the subscribing device (Fig 5A; col 4, lines 25-27; col 4, lines 33-41).

Re claim 14: D'Amico teaches the stored mapping of the secret identifier is the subscription information encrypted with the secret identifier as encryption key (col 1, lines 44-52).

Re claim 15: D'Amico teaches a subscription authority device [Fig 1, elts 12 & 14; Fig 3; "BASE STATION" / "network operator"] for secure device subscription, characterized in that the subscription authority device [Fig 1, elts 12 & 14; Fig 3; "BASE STATION" / "network operator"] is arranged to implement a first-time subscription protocol (Fig 4: col 2, lines 15-17), during which it receives a mapping of a secret identifier of a subscribing device [Fig 1, elt 16: "SUSBSCRIBER UNIT"], the subscription authority device [Fig 1, elts 12 & 14; Fig 3; "BASE STATION" / "network operator"] is arranged to store the mapping of the secret identifier (col 1, lines 43-52), the subscription authority device is further arranged to implement a renewed subscription protocol (Fig 5: col 2, lines 18-19), during which it uses the stored mapping of the secret identifier (col 4, lines 36-41).

Re claim 16: D'Amico teaches a subscribing device [Fig 1, elt 16: "SUSBSCRIBER UNIT"] to participate in a network requiring subscription, characterized in that the subscribing device is arranged to contain a public identifier ["portable identification number"] and a secret identifier ["key code"], the subscribing device is further arranged to implement a first-time subscription protocol (Fig 4: col 2, lines 15-17) during which it transmits a mapping of the secret identifier protocol (col 1, lines 43-52) and during which it receives subscription information (col 3, lines 10-18), the subscribing device is further arranged to implement a renewed subscription protocol [Fig 5a, elt 202]

(col 4, lines 36-41), during which it receives subscription information which requires the secret identifier for decryption (col 3, lines 4-10).

Re claim 17: D'Amico teaches a system for secure device subscription (Fig 1), the system comprising a subscribing device [Fig 1, elt 16: "SUSBSCRIBER UNIT"] is described in claim 16 (claim 16 is addressed *supra*), and a subscription authority device [Fig 1, elts 12 & 14; Fig 3; "BASE STATION" / "network operator"] is described in claim 15 (claim 15 is addressed *supra*).

Re claim 19: D'Amico teaches a router device that is in connection with the subscribing device acts as the subscription authority (Figs 1 & 3; col 2, lines 25-26; col 2, lines 40-47).

Re claim 20: D'Amico teaches the router device acts as an independent subscription authority (Figs 1 & 3; col 2, lines 25-26; col 2, lines 40-47).

Re claim 21: D'Amico teaches a router device from a group of router devices may act as a virtual single subscription authority (Figs 1 & 3; col 2, lines 25-26; col 2, lines 40-47; a group of one device meets the claim).

Re claim 22: D'Amico teaches the subscribing device communicates local data to the subscription authority, and the subscription authority stores the local data (col 1, lines 44-52).

Re claim 23: D'Amico teaches the subscribing device retrieves at least part of the stored local data from the subscription authority (col 2, lines 35-39; col 4, lines 25-44).

Re claim 24: D'Amico teaches the subscribing device encrypts local data using the secret identifier as encryption key, the subscribing device subsequently

communicates the encrypted local data to the subscription authority, and the subscription authority stores the encrypted local data (col 1, lines 41-52; the Examiner notes that choosing to store credentials in its unencrypted form or encrypted form is a matter of choice and is fully encompassed by the prior art).

Re claim 25: D'Amico teaches the subscribing device encrypts local data using the secret identifier as encryption key, the subscribing device subsequently communicates the encrypted local data to the subscription authority, and the subscription authority decrypts the encrypted local data and stores the decrypted local data (col 1, lines 41-52; the Examiner notes that choosing to store credentials in its unencrypted form or encrypted form is a matter of choice and is fully encompassed by the prior art).

2. Claim 18 is rejected under 35 U.S.C. 102(b) as being anticipated by Nakakita et al (U.S. Pat App Pub 2002/0061748 A1), hereinafter referred to as Nakakita.

Re claim 18: Nakakita teaches a signal for secure device subscription (Fig 3: ¶26), characterized in that the signal [Fig 3, elt 5] carries a mapping [Fig 6] of a secret identifier [Fig] of a subscribing device [Fig 3 , elt "TERMINAL 1"] (¶70).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 2, 3, 6, 26 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over D'Amico et al (U.S. Pat 5077790 A), hereinafter referred to as D'Amico, in view of Akashi (U.S. Pat App Pub 2002/0026424 A1), hereinafter referred to as Akashi.

Re claim 2: D'Amico teaches all the limitations of claim 1 as previously stated and further teaches the first-time subscription protocol (Fig 4: col 2, lines 15-17).

However, Akashi teaches subscription authority [Fig 6, elt 200: "License issuing device"] and subscribing device commonly [Fig 6, elt 100: "Memory card"] and securely obtain a value r [R2] (Fig 4, elts ST401 & ST402: ¶77-¶78; Fig 6, elts ST613 & ←R2--: ¶102), the subscribing device subsequently encrypts the value r using the secret identifier as encryption key (Fig 6, elt ST605; ¶95; ¶104), and the subscribing device subsequently communicates the encrypted value [Fig 6, elt --E1r2→] to the subscription authority (¶104).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of D'Amico with the teachings of Akashi, for the purpose of mutually verifying two communicating parties comprise a common secret while protecting said common secret, as taught by Akashi.

Re claim 3: The combination of D'Amico and Akashi teaches during execution of the first-time subscription protocol the subscription authority generates the value r, and the subscription authority communicates the value r securely to the subscribing device (Akashi: Fig 4, elts ST401 & ST402; Fig 6, elt ST613; ¶102).

Re claim 6: The combination of D'Amico and Akashi teaches the renewed subscription protocol (D'Amico: Fig 5: col 2, lines 18-19); subscription authority communicates the value r encrypted with the secret identifier as encryption key to the subscribing device (Akashi: Fig 6, elts ST611, ST612 & ←E2r1--).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of D'Amico with the teachings of Akashi, for the purpose of securely identifying and securely communicating between parties, as taught by Akashi.

Re claim 12: D'Amico teaches all the limitations of claim 1 as previously stated. However, Akashi teaches the first-time subscription protocol the subscription authority communicates the subscription information securely to the subscribing device, the subscribing device subsequently encrypts the subscription information using the secret identifier as encryption key (Fig 6, elts ST611 & ST 612), and the subscribing device subsequently communicates the encrypted subscription information to the subscription authority (Fig 6, elts ST605 & --E1r2→).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of D'Amico with the teachings of Akashi, for the purpose of securely identifying and securely communicating between parties, as taught by Akashi.

Re claim 26: The combination of D'Amico and Akashi teaches the subscribing device [Akashi: Fig 6, elt 100] encrypts local data using the value r as encryption key, the subscribing device subsequently communicates the encrypted local data to the

subscription authority [Akashi: Fig 6, elt 200], and the subscription authority stores the encrypted local data (Akashi: Fig 6, elts ST611 & ST612; the Examiner notes that choosing to store credentials in its unencrypted form or encrypted form is a matter of choice and is fully encompassed by the prior art).

Re claim 27: The combination of D'Amico and Akashi teaches the subscribing device [Akashi: Fig 6, elt 100] encrypts local data using the value r as encryption key, the subscribing device subsequently communicates the encrypted local data to the subscription authority [Akashi: Fig 6, elt 200], and the subscription authority decrypts the encrypted local data and stores the decrypted local data (Akashi: Fig 6, elts ST611 & ST612; the Examiner notes that choosing to store credentials in its unencrypted form or encrypted form is a matter of choice and is fully encompassed by the prior art).

4. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over D'Amico et al (U.S. Pat 5077790 A), hereinafter referred to as D'Amico, in view of Akashi (U.S. Pat App Pub 2002/0026424 A1), hereinafter referred to as Akashi, in further view of Applicant's Admitted Prior Art, hereinafter referred to as AAPA.

Re claim 4: The combination of D'Amico and Akashi teaches all the limitations of claim 2 as previously stated. However, AAPA teaches the first-time subscription protocol the subscription authority and subscribing device commonly generate a value r using a secure common key generation protocol (page 8, lines 11-16).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of D'Amico and Akashi with the

teachings of AAPA, for the purpose of security establishing an encryption key between communicating parties without actually transmitting the key between communication parties and averting man-in-the-middle attacks, as taught by the Diffie-Hellman key establishment and Shamir's "no-key" protocols.

5. Claims 5, 7 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over D'Amico et al (U.S. Pat 5077790 A), hereinafter referred to as D'Amico, in view of Akashi (U.S. Pat App Pub 2002/0026424 A1), hereinafter referred to as Akashi, in further view of Nakakita et al (U.S. Pat App Pub 2002/0061748 A1), hereinafter referred to as Nakakita.

Re claim 5: The combination of D'Amico and Akashi teaches all the limitations of claim 2 as previously stated. However, Nakakita teaches during execution of any of the subscription protocols the subscription authority encrypts the subscription information using the value r as encryption key, and the subscription authority subsequently communicates the encrypted subscription information to the subscribing device (Fig 6; ¶82-¶83).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of D'Amico and Akashi with the teachings of Nakakita, for the purpose of securely providing network secrets to facilitate secure communication between parties, as taught by Nakakita.

Re claim 7: The combination of D'Amico and Akashi teaches all the limitations of claim 2 as previously stated. However, Nakakita teaches the stored mapping of the

secret identifier is the value r, encrypted with the secret identifier as encryption key (Fig 9; ¶32).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of D'Amico and Akashi with the teachings of Nakakita, for the purpose of securely providing network secrets to facilitate secure communication between parties, as taught by Nakakita.

Re claim 8: The combination of D'Amico, Akashi and Nakakita teaches the value r is also stored by the subscription authority (Fig 9; ¶32).

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 7am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. S./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435